Quiz: Lab Security Audit

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the Checks-Effects-Interactions pattern designed to prevent?
A) Integer overflow B) Reentrancy attacks C) Oracle manipulation D) Access control

Quiz (1–5)

Q1. What is the Checks-Effects-Interactions pattern designed to prevent?
A) Integer overflow B) Reentrancy attacks C) Oracle manipulation D) Access control
Answer: B – Update state before external calls to prevent reentrant exploitation.

Q2. Which Solidity version introduced built-in overflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0 D) 0.9.0

Quiz (1–5)

Q1. What is the Checks-Effects-Interactions pattern designed to prevent?
A) Integer overflow B) Reentrancy attacks C) Oracle manipulation D) Access control
Answer: B – Update state before external calls to prevent reentrant exploitation.

Q2. Which Solidity version introduced built-in overflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0 D) 0.9.0
Answer: C – Solidity 0.8.0+ automatically reverts on arithmetic overflow.

Q3. What severity is assigned to reentrancy enabling fund drainage?
A) Low B) Medium C) High D) Critical

Quiz (1–5)

Q1. What is the Checks-Effects-Interactions pattern designed to prevent?
A) Integer overflow B) Reentrancy attacks C) Oracle manipulation D) Access control
Answer: B – Update state before external calls to prevent reentrant exploitation.

Q2. Which Solidity version introduced built-in overflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0 D) 0.9.0
Answer: C – Solidity 0.8.0+ automatically reverts on arithmetic overflow.

Q3. What severity is assigned to reentrancy enabling fund drainage?
A) Low B) Medium C) High D) Critical
Answer: D – Direct fund theft vulnerabilities are Critical severity.

Q4. Which tool uses symbolic execution for deep analysis?
A) Slither B) Mythril C) Hardhat D) Truffle

Quiz (1–5)

Q1. What is the Checks-Effects-Interactions pattern designed to prevent?
A) Integer overflow B) Reentrancy attacks C) Oracle manipulation D) Access control
Answer: B – Update state before external calls to prevent reentrant exploitation.

Q2. Which Solidity version introduced built-in overflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0 D) 0.9.0
Answer: C – Solidity 0.8.0+ automatically reverts on arithmetic overflow.

Q3. What severity is assigned to reentrancy enabling fund drainage?
A) Low B) Medium C) High D) Critical
Answer: D – Direct fund theft vulnerabilities are Critical severity.

Q4. Which tool uses symbolic execution for deep analysis?
A) Slither B) Mythril C) Hardhat D) Truffle
Answer: B – Mythril explores execution paths; Slither uses fast static analysis.

Q5. What does TWAP stand for in oracle security?
A) Time-Weighted Average Price B) Total Weighted Asset Pool C) Trustless Web API D) Two-Way Auth

Quiz (1–5)

Q1. What is the Checks-Effects-Interactions pattern designed to prevent?
A) Integer overflow B) Reentrancy attacks C) Oracle manipulation D) Access control
Answer: B – Update state before external calls to prevent reentrant exploitation.

Q2. Which Solidity version introduced built-in overflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0 D) 0.9.0
Answer: C – Solidity 0.8.0+ automatically reverts on arithmetic overflow.

Q3. What severity is assigned to reentrancy enabling fund drainage?
A) Low B) Medium C) High D) Critical
Answer: D – Direct fund theft vulnerabilities are Critical severity.

Q4. Which tool uses symbolic execution for deep analysis?
A) Slither B) Mythril C) Hardhat D) Truffle
Answer: B – Mythril explores execution paths; Slither uses fast static analysis.

Q5. What does TWAP stand for in oracle security?
A) Time-Weighted Average Price B) Total Weighted Asset Pool C) Trustless Web API D) Two-Way Auth
Answer: A – TWAP averages prices over time to resist manipulation.

Quiz (6–10)

Q6. What is the main risk of using Uniswap spot prices?
A) High gas B) Flash loan manipulation C) Slow execution D) Protocol fees

Quiz (6–10)

Q6. What is the main risk of using Uniswap spot prices?
A) High gas B) Flash loan manipulation C) Slow execution D) Protocol fees
Answer: B – Spot prices can be manipulated within a single transaction.

Q7. Which OpenZeppelin contract prevents reentrancy?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl

Quiz (6–10)

Q6. What is the main risk of using Uniswap spot prices?
A) High gas B) Flash loan manipulation C) Slow execution D) Protocol fees
Answer: B – Spot prices can be manipulated within a single transaction.

Q7. Which OpenZeppelin contract prevents reentrancy?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl
Answer: C – ReentrancyGuard provides the nonReentrant modifier.

Q8. What is SWC-107 in the weakness registry?
A) Integer overflow B) Reentrancy C) Access control D) Denial of service

Quiz (6–10)

Q6. What is the main risk of using Uniswap spot prices?
A) High gas B) Flash loan manipulation C) Slow execution D) Protocol fees
Answer: B – Spot prices can be manipulated within a single transaction.

Q7. Which OpenZeppelin contract prevents reentrancy?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl
Answer: C – ReentrancyGuard provides the nonReentrant modifier.

Q8. What is SWC-107 in the weakness registry?
A) Integer overflow B) Reentrancy C) Access control D) Denial of service
Answer: B – SWC-107 specifically identifies reentrancy vulnerabilities.

Q9. What is the correct order in Checks-Effects-Interactions?
A) Effects, Checks, Interactions B) Interactions, Effects, Checks C) Checks, Effects, Interactions D) Checks, Interactions, Effects

Quiz (6–10)

Q6. What is the main risk of using Uniswap spot prices?
A) High gas B) Flash loan manipulation C) Slow execution D) Protocol fees
Answer: B – Spot prices can be manipulated within a single transaction.

Q7. Which OpenZeppelin contract prevents reentrancy?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl
Answer: C – ReentrancyGuard provides the nonReentrant modifier.

Q8. What is SWC-107 in the weakness registry?
A) Integer overflow B) Reentrancy C) Access control D) Denial of service
Answer: B – SWC-107 specifically identifies reentrancy vulnerabilities.

Q9. What is the correct order in Checks-Effects-Interactions?
A) Effects, Checks, Interactions B) Interactions, Effects, Checks C) Checks, Effects, Interactions D) Checks, Interactions, Effects
Answer: C – Validate, update state, then make external calls.

Q10. Why write exploit contracts during audits?
A) Increase fees B) Prove vulnerability severity C) Test compiler D) Generate docs

Quiz (6–10)

Q6. What is the main risk of using Uniswap spot prices?
A) High gas B) Flash loan manipulation C) Slow execution D) Protocol fees
Answer: B – Spot prices can be manipulated within a single transaction.

Q7. Which OpenZeppelin contract prevents reentrancy?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl
Answer: C – ReentrancyGuard provides the nonReentrant modifier.

Q8. What is SWC-107 in the weakness registry?
A) Integer overflow B) Reentrancy C) Access control D) Denial of service
Answer: B – SWC-107 specifically identifies reentrancy vulnerabilities.

Q9. What is the correct order in Checks-Effects-Interactions?
A) Effects, Checks, Interactions B) Interactions, Effects, Checks C) Checks, Effects, Interactions D) Checks, Interactions, Effects
Answer: C – Validate, update state, then make external calls.

Q10. Why write exploit contracts during audits?
A) Increase fees B) Prove vulnerability severity C) Test compiler D) Generate docs
Answer: B – Exploit PoCs demonstrate real attack scenarios.